IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

In re Patent Application of: **LAWTON ET AL.**	
Serial No. **10/669,097**	Examiner: **April Y. SHAN**
Filing Date: **SEPTEMBER 23, 2003** Confirmation No: **1842**	Art Unit: **2135**
For: **METHOD FOR SETTING AN ENCRYPTION KEY FOR LOGICAL NETWORK SEPARATION**	Attorney Docket No. 32250

APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief together with the requisite $255.00 small entity fee for filing a brief. If any additional extension and/or fee is required, authorization is given to charge Deposit Account No. **01-0484**.

(1) Real Party in Interest

The real party in interest is Intellon Corporation, assignee of the present application as recorded at reel 014982, frame 0359.

(2) Related Appeals and Interferences

None.

(3) Status of the Claims

Claims 1-10 are pending in the application. Claim 1 is the only independent claim. Claims 1-10 stand rejected. Applicants appeal the rejection of all pending claims.

(4) Status of the Amendments

There are no outstanding amendments. No amendments were filed after the Final Office Action of December 20, 2007.

(5) Summary of the Claimed Subject Matter

The present invention is directed a method for determining MAC (Media Access Control) address for a remote device (see, e.g., Figure 1, "Node A") having a known, unique DEK (Device Encryption Key) in a network (see, e.g, Figure 1, "Logical Network 1") where devices may not send a confirmation to a *SetNEK* (Set Network Encryption Key) request. According to independent claim 1, the method comprises the steps of:

preparing a broadcast message with a *SetNEK* request containing a unique, temporary *NEK* (see, e.g., paragraph [0026], step 1 of "Procedure B");

encrypting the message with the DEK of the remote device (see, e.g., id);

transmitting the broadcast message on a network medium (see, e.g., id);

confirming receipt of the temporary *NEK* by sending a request that requires a response from the remote device which is encrypted with the temporary *NEK* (see, e.g., paragraph [0026], step 2 of "Procedure B"); and

determining the MAC address of the remote device from the response (see, e.g., paragraph [0026], steps 3 and 4 of "Procedure B").

Applicants note that a helpful discussion of terminology used in connection with logical networks can be found in paragraphs [0005] – [0014] of Applicants' Specification.

(6) Grounds of Rejection to be Reviewed On Appeal

Applicants respectfully request review of the rejection of claims 1-10 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,987,770 to Yonge, III ("Yonge").

(7) Argument

As will be described in greater detail below, Applicants respectfully submit that the outstanding ground of rejection is improper, and should be reversed, at least because Yonge does not show or disclose each and every recitation of Applicants' claim 1.

Accordingly, and in view of the following detailed arguments, Applicants respectfully request that the rejection of claims 1-10 be reversed.

CLAIMS 1-10 ARE NOT PROPERLY REJECTED UNDER 35 U.S.C. § 102(e) AS ANTICIPATED BY YONGE

The Examiner rejected claim 1 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,987,770 to Yonge, III ("Yonge"). An anticipation rejection under § 102 is improper unless a single prior art reference shows or discloses each and every claim recitation, as arranged in the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990); *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); see generally, MPEP 2131.

CLAIMS 1-10

Applicants' claim 1 recites a method for determining MAC address for a remote device having a known, unique DEK in a network where devices may not send a confirmation to a *SetNEK* request, the method comprising the steps of preparing a broadcast message with a *SetNEK* request containing a unique, temporary NEK, encrypting the message with the DEK of the remote device, transmitting the broadcast message on a network medium, confirming receipt of the temporary NEK by sending a

request that requires a response from the remote device which is encrypted with the temporary NEK, and determining the MAC address of the remote device from the response. Applicants' claims 2-10 depend, directly or indirectly, from claim 1 and include additional recitations thereto.

Yonge clearly does not show or disclose each and every recitation of Applicants' claim 1. For instance, Yonge does not show or disclose preparing a broadcast message with a *SetNEK* request containing a *unique, temporary* NEK. Instead, Yonge discloses:

> A station that is already a member of the logical network, or "master" station receives the default key of the new station. Typically, the default key of the new station is manually entered into the master station. The master station builds a frame that includes a Set Network Encryption Key MAC Management Entry, the entry identifying a 56-bit DES Network Encryption Key or NEK and an associated 8-bit Encryption Key Selection ***for the logical network***. (Yonge, col. 33, lines 35-45; internal citations omitted; emphasis added.)

Thus, Yonge expressly discloses that the Set Network Encryption Key MAC Management Entry (*SetNEK* MME) contains the NEK ***for the logical network***. This is the same NEK shared by all the other devices on the logical network and used repeatedly for transactions in the logical network (see, e.g, Yonge, col. 33, line 63 – col. 34, line 3), and is, therefore, neither *unique* nor *temporary*.

The Yonge procedure for adding a new station to the logical network is effectively the same as step 1 of "Procedure A", described in paragraph [0017] of the "BACKGROUND" section of Applicants' Specification, where a new station is added (or an existing station is moved) to a logical network by simply sending the NEK for the logical network in an initial *SetNEK* request. Yonge does not show or disclose any intervening steps of preparing and transmitting a *SetNEK* request containing a unique, temporary NEK, in stark contrast to Applicants' claim 1.

Thus, Yonge does not show or disclose each and every recitation of

Applicants' claim 1. Accordingly, Applicants respectfully submit that the rejection of claim 1 under 35 U.S.C. § 102(e) as anticipated by Yonge is improper for at least this reason, and should be reversed.

CLAIM 4

Applicants' claim 4 depends indirectly from claim 1 and additionally recites the step of using the MAC address of the remote device in a unicast transmission containing a *SetNEK* message with the local NEK (the NEK for the network to which the remote device is to be added or moved). Yonge does not show or disclose these additional recitations. In fact, the additional recitations of claim 4 help to highlight the impropriety of the claim 1 rejection. In the Yonge procedure, the NEK ***for the logical network*** is initially transmitted to the new station with the *SetNEK* MME. Thus, the local NEK has *already* been transmitted to the new station. Therefore, if the NEK for the logical network were sent again in a redundant *SetNEK* MME (which Yonge does not actually appear to show or disclose doing), it would be the *same* NEK that was transmitted initially. Accordingly, this NEK could not be properly interpreted as disclosing *both* the unique, temporary NEK *and* the local NEK recited by Applicants' claims 1 and 4.

Thus, Yonge does not show or disclose the additional recitations of Applicants' claim 4. Accordingly, Applicants respectfully submit that the rejection of claim 4 under 35 U.S.C. § 102(e) as anticipated by Yonge is further improper for at least this reason.

CONCLUSIONS

In view of the foregoing arguments, it is submitted that all of the claims are patentable over the prior art. Accordingly, the Board of Patent Appeals and

Interferences is respectfully requested to reverse the earlier unfavorable decision by the Examiner.

Respectfully submitted,

JUSTIN R. SAUER, ESQ.
Reg. No. 56,920
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Appellant

APPENDIX A - CLAIMS ON APPEAL FOR U.S. PATENT APPLICATION SERIAL NO. 10/669,097

1. (Original) A method for determining MAC address for a remote device having a known, unique DEK in a network where devices may not send a confirmation to a *SetNEK* request, the method comprising the steps of:

preparing a broadcast message with a *SetNEK* request containing a unique, temporary *NEK*;

encrypting the message with the DEK of the remote device:

transmitting the broadcast message on a network medium;

confirming receipt of the temporary *NEK* by sending a request that requires a response from the remote device which is encrypted with the temporary *NEK*; and

determining the MAC address of the remote device from the response.

2. (Original) The method of Claim 1 wherein the remote device is not a member of a network.

3. (Original) The method of Claim 2 further comprising the step of using the MAC address of the remote device in a unicast transmission to reliably confirm receipt of the temporary *NEK*.

4. (Original) The method of Claim 3 further comprising the step of using the MAC address of the remote device in a unicast transmission containing a *SetNEK* message with the local NEK.

5. (Original) The method of Claim 4 further comprising the step of using the MAC address of the remote device in an additional unicast transmission which is encrypted with the local *NEK*, for purposes of confirming receipt of the local *NEK*.

6. (Original) The method of Claim 2 further comprising the steps of:

using the determined MAC address to reliably send the local *NEK*;

preparing a unicast message to the remote device containing a *SetNEK* request where the *SetNEK* request contains a unique, temporary *NEK*;

encrypting the unicast message with the DEK of the remote device;

transmitting the unicast message on the medium; and

confirming receipt of the temporary *NEK* by sending a request that requires a response which is encrypted with the temporary *NEK*.

7. (Original) The method recited in Claim 1, wherein the network is a powerline network.

8. (Original) The method recited in Claim 1, wherein the remote devices are implemented according to the HomePlug Powerline Alliance standard.

9. (Original) The method of Claim 1 wherein the request is a request statistics MME and the response is a statistic response MME.

10. (Original) The method of Claim 1 wherein the request is a request channel estimation MME and the response is a channel estimation response.

APPENDIX B – EVIDENCE APPENDIX
PURSUANT TO 37 C.F.R. § 41.37(c)(1)(ix)

None.

APPENDIX C – RELATED PROCEEDINGS APPENDIX
PURSUANT TO 37 C.F.R. § 41.37(c)(1)(x)

None.